Table of Contents

Introduction

This Privacy Impact Assessment (PIA) is an assessment conducted by Newport City Council to help the organisation identify and reduce the privacy risks associated with the provision of the public WiFi service. The Assessment provides an audit of the systems processes and examines how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes.

This PIA is designed to accomplish three goals:

- Ensure compliance with applicable legal, regulatory, and policy requirements for privacy;
- Determine the risks and effects; and
- Evaluate protections and alternative processes to mitigate potential privacy risks.

This document has been produced with the intention that it be transparent and open to public scrutiny. The assessment demonstrates that we have examined the integrity of the public WiFi system and provides confidence to those seeking assurance, that their personal data is protected.

Annex one

Privacy Impact Assessment Screening Questions.

These questions are intended to help organisations decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to. You can adapt these questions to develop a screening method which fits more closely with the types of project you are likely to assess.

Will the project involve the collection of new information about individuals?
Yes. The end user portal will provide a single registration process for all locations. The End-User Portal shall include authentication and tracking facilities as part of the WiFi Network to ensure End-Users are authenticated using one of the available social media or form based options prior to being able to access the Internet. The current options available include – Facebook, LinkedIn, Twitter, Google+, Instagram and any electronic form based registration process

Will the project compel individuals to provide information about themselves?
Yes. Log-in information (name and e-mail address) and/or information from social media account if this is the chosen method of log-in. Device and location data is stored to ensure appropriate legislation is complied with and to enhance the WiFi service.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
Yes. The End-User portal shall provide End-Users with the ability to opt-in to receive targeted communication (including special offers and marketing material) from the Service Provider. The Service Provider shall ensure that the End-User Portal presentation of the targeted communication opt-in is clear to all End-Users. The Service Provider shall also ensure that End-Users have the option to change their preferences in respect of future use of End User Data. Public buildings and City Centre WiFi service will share the same infrastructure. A separate infrastructure will exist for bus services. There is no plan to push advertising, on the transport service, however, surveys will potentially be introduced in the future. Tracking, mac address and bus location (AP).

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
Yes. See above.

Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
Yes. Device Information and location may be used in conjunction with submitted information and treated as personal data for this purpose. Actual location information may be collected and processed.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
No.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
The monitoring of location data may be perceived as intrusive.

Will the project require you to contact individuals in ways which they may find intrusive?
Where the user has opted to receive marketing information via the portal, they will only be contacted by electronic means (e-mail or SMS). The end user may opt out at any time and the communication will stop.

Annex two

Step one: Identify the need for a PIA

Newport has aspirations to be one of the leading Digital Cities in the UK ultimately to increase wealth and job creation across the City. The vision for a Future Newport is a city of technology, sport and culture with an international profile which will encourage and drive economic growth, innovation and prosperity. To help achieve this there is a need to develop an infrastructure that supports future internet technologies and facilitates new public sector service delivery models.

PROJECT OBJECTIVES

The Council wishes to select a suitably qualified and experienced Tenderer to design, deploy and operate a Managed Wi-Fi Service across its property portfolio

Grant funding is available for wireless infrastructure and network connectivity from the Super Connected Cities programme to fund capital investment

Upon completion of a successful procurement process, the Council intends to award a 3 year contract (with options for further extension) to the Tenderer

The specific objective within this project are to establish WIFI within public sector building within the city's boundaries to enable customers to

- Access digital by default services and information.
- Enjoy the city's cultural facilities
- Increase digital engagement between the public, the government and ourselves
- Allow consumer and business users to be online when they are away from their home or the office
- Encourage visitors to stay in the city for longer
- Promote Newport as a city on the rise
- There are also potential opportunities around utilising the Wi-Fi network as a distribution channel for marketing content.

The Service will be

- Affordable for the customer to use.
  - An Open Network that provides an opportunity to connect to services provided by commercial Mobile network operators.
  - Future proof and capable of expansion to allow access to 4G services and beyond.
  - As unified as possible – with the ability to switch from different wireless providers
- Maximises speed and bandwidth capacity.
  - Maximises private sector investment, acknowledging the public sector role as an enabler but recognizing that the private sector is best placed to deliver.
  - Supports the Council's Prospectus for Change agenda and the reNewport report from the Newport Business Development Task Force to Welsh Government

Why is a PIA required? (summary of screening questions in Annex 1)

Will the project involve the collection of new information about individuals?
Yes. The end user portal will provide a single registration process for all locations. The End-User Portal shall include authentication and tracking facilities as part of the WiFi Network to ensure End-Users are authenticated using one of the available social media or form based options prior to being

able to access the Internet. The current options available include – Facebook, LinkedIn, Twitter, Google+, Instagram and any electronic form based registration process

Will the project compel individuals to provide information about themselves?
Yes. Log-in information (name and e-mail address) and/or information from social media account if this is the chosen method of log-in. Device and location data is stored to ensure appropriate legislation is complied with and to enhance the WiFi service.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
Yes. The End-User portal shall provide End-Users with the ability to opt-in to receive targeted communication (including special offers and marketing material) from the Service Provider. The Service Provider shall ensure that the End-User Portal presentation of the targeted communication opt-in is clear to all End-Users. The Service Provider shall also ensure that End-Users have the option to change their preferences in respect of future use of End User Data. Public buildings and City Centre WiFi service will share the same infrastructure. A separate infrastructure will exist for bus services. There is no plan to push advertising, on the transport service, however, surveys will potentially be introduced in the future. Tracking, mac address and bus location (AP).

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
Yes. See above.

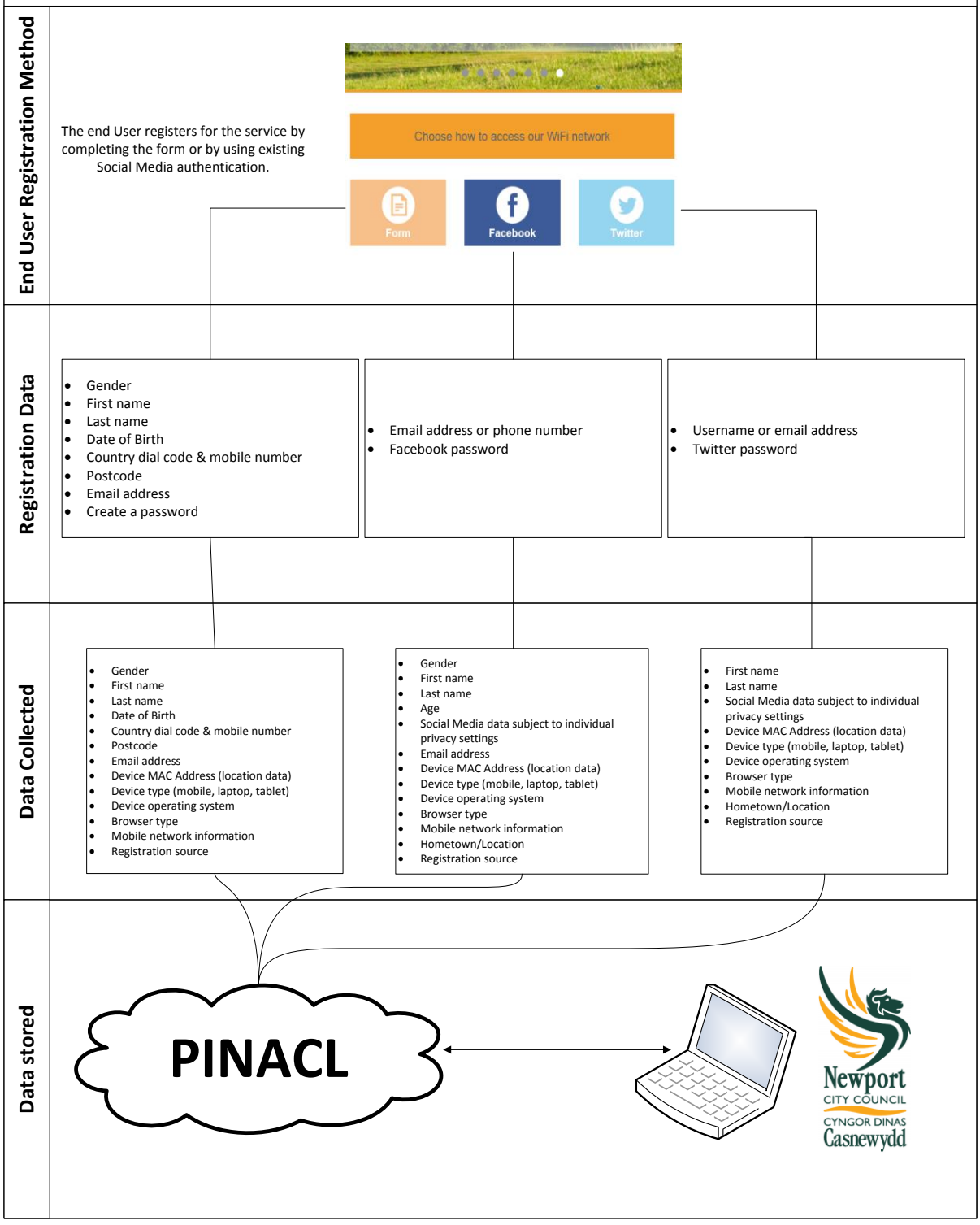
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
Yes. Device Information and location may be used in conjunction with submitted information and treated as personal data for this purpose. Actual location information may be collected and processed.

Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?
No.

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly private.
The monitoring of location data may be perceived as intrusive.

Will the project require you to contact individuals in ways which they may find intrusive?
Where the user has opted to receive marketing information via the portal, they will only be contacted by electronic means (e-mail or SMS). The end user may opt out at any time and the communication will stop.

Annex Three, Data Flow, Registration and Authentication Process.

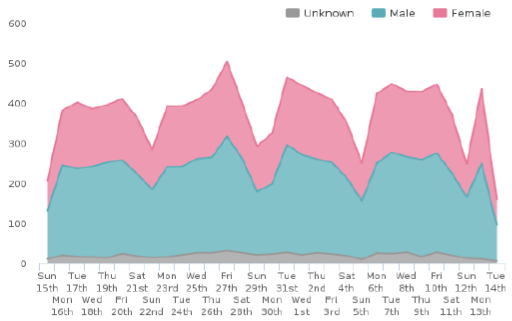


How The Data Is Used – Usage Reports.

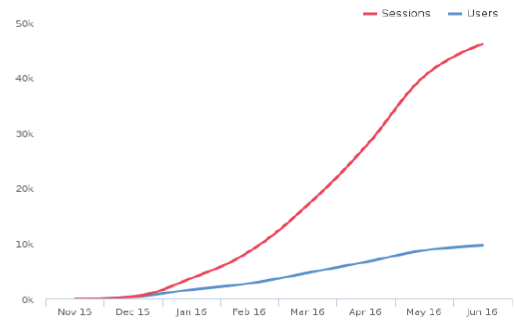
PINACL
UNLOCKING POSSIBILITIES THROUGH ICT

Overview
Between 7th Jun 2016 and 14th Jun 2016

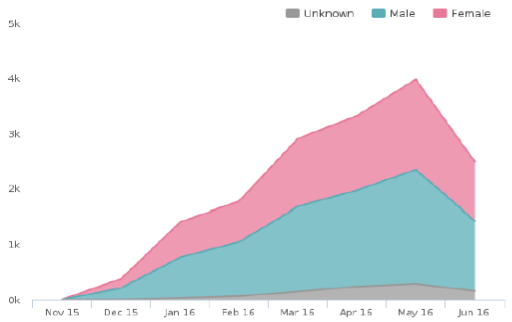
Users by day



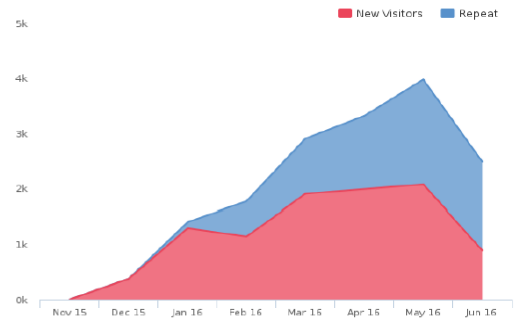
Cumulative users and sessions



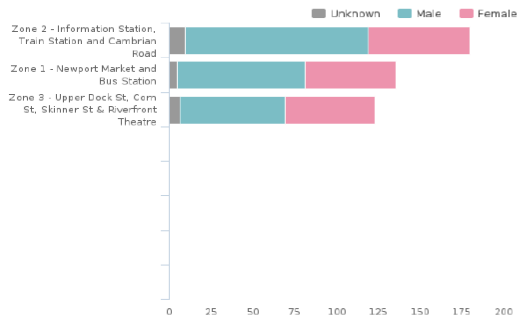
Users by month



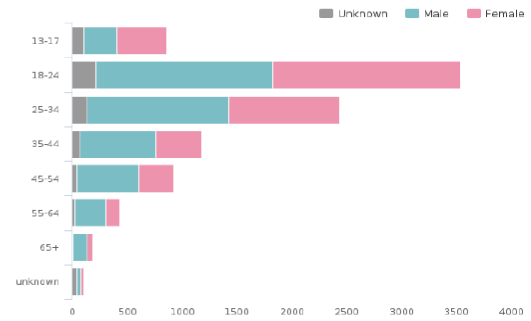
Users by month (new vs repeat)



Top venues by daily average (last 28 days)



User demographics



Newport CityConnect

PINACL
UNLOCKING POSSIBILITIES THROUGH ICT

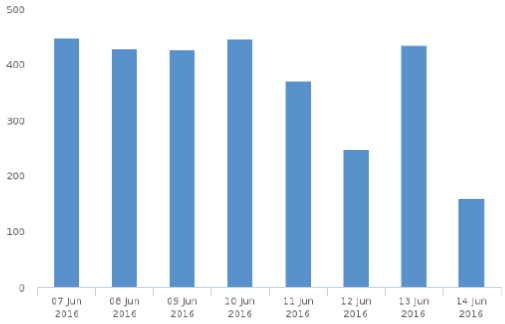
Visitor Reports

Between 7th Jun 2016 and 14th Jun 2016

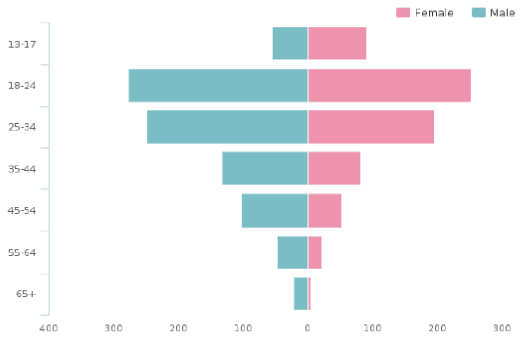
Total WiFi users

	New Users	Repeat Users	Unique Users
Registration Form	248	583	781
Facebook	212	677	843
Twitter	31	47	72

WiFi users by day

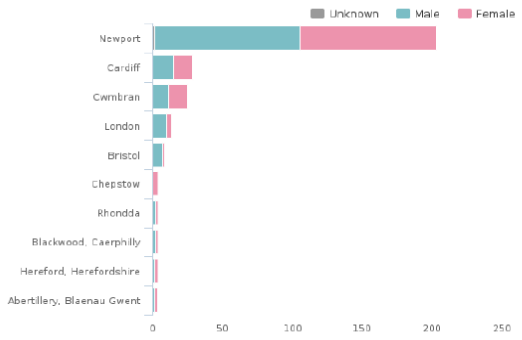


WiFi user demographics

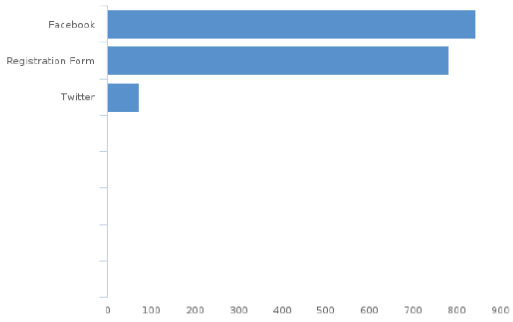


Age

Top 10 visitor locations



Visitor sources

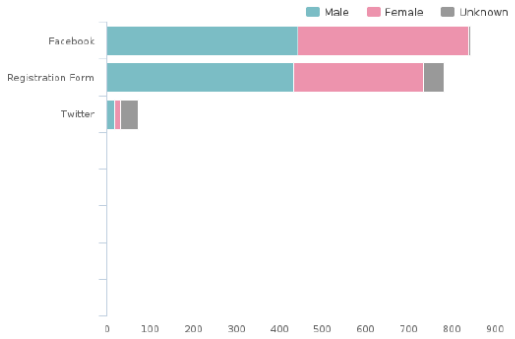


Newport CityConnect

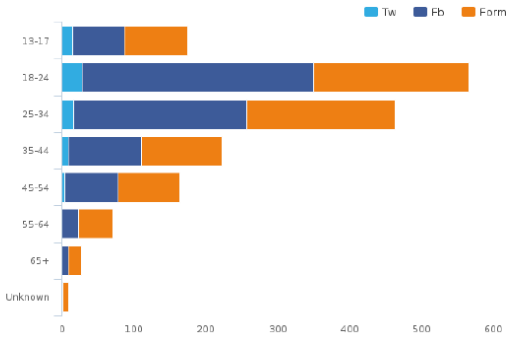
PINACL
UNLOCKING POSSIBILITIES THROUGH ICT

Visitor Reports
Between 7th Jun 2016 and 14th Jun 2016

Social networks by gender



Social networks by age



Wi-Fi Access Points in the City Centre

There are currently 19 of the 22 Access Points installed and operational, please see illustration below:

- Underside of CCTV bracket at the rear right corner on Market Building - **1**
- Lamppost opposite Bay 19 in the Bus station (no asset ID) - **2**
- Lamppost outside Waris store (NL186) - **3**
- Lamppost outside Tenovus store (NL212) - **4**
- Lamp on Vodafone Store (NL779) - **5**
- Lamppost outside Impact store (NL1015) - **6**
- The front right corner of the Information Station - **7**
- Lamppost next to pedestrian crossing (NL11B) - **8**
- Lamppost outside the Grey Hound (NL237) - **9**
- Lamppost outside the Panasonic Store (NL237) - **10**
- Lamppost on Queensway (NL04A) - **11**
- Lamppost on Queensway (NL08A) - **12**
- Lamppost opposite Yates (NL203) - **13**
- On Citizens Advice Bureau building - **14**
- Lamppost (NL39) - **15**
- On Citizens Advice Bureau building - **16**
- Lamppost on A4042 (NL600) - **17**
- Lamppost opposite Market Street (NL156) - **18**
- Lamppost outside Market Arcade (NL195) – **19**


Stanley Rd
A4042
New Bus Station
Cambrian Rd
Station St
Skinner St
Skinner Ln
Bridg
Upper Dock St
B4597
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

Wi-Fi Access Points in Buildings (Wi-Fi is only available in the public areas of the buildings)

Annex four

Step three: identify the privacy and related risks

Community Cloud or City Connect?	Privacy Issue:	Risk to Individuals:	Compliance Risk:	Associated Corporate:
Both	Personal data of approximately 20,000 individuals stored in the cloud. Data items detailed in Annex 3. No sensitive personal data as defined by the DPA 1998.	Whole dataset could be hacked.	Breach DPA, Principle 7.	Reputational damage. Potential monetary penalty. Lack of trust in the organisation as a result.
Both	Where is the data stored? Need to consider the security and location of the data centre or centres.	Concerns as to Principle 8, data storage outside of EEA and Principle 7, security.	Breach DPA, Principles 7 & 8.	Reputational damage. Potential monetary penalty. Lack of trust in the organisation as a result.
Both	Location of an individual's device could be derived. This data is available historically and in real time.	Potentially, an individual's location over time could be tracked.	Breach DPA, Principle 7.	Reputational damage. Potential monetary penalty. Lack of trust in the organisation as a result.
Both	How long is the data stored and what process is there to destroy?	Potentially a breach of Principle 5, retention. Also, correct disposal method must be employed, Principle 7.	Breach DPA, Principle 5 & 7.	Potential monetary penalty. Lack of trust in the organisation as a result.

Both	Information recorded may be shared with law enforcement, governmental agencies and other authorities.	Exemptions under the DPA allow for this sharing to happen. The perception may be that we are misusing customer data.	Breach DPA, Principle 7.	Reputational damage. Lack of trust in the organisation as a result.
Both	The information gathered could be used by the service provider to communicate with the device holder.	The device holder may receive communication which is subsequently unwanted.	PECR	Reputational damage. Lack of trust in the organisation as a result.
Both	The information stored could be sold on to a third party. Could be shared with other areas of the company/group of companies.	The device holder may receive communication which is subsequently unwanted.	PECR	Reputational damage. Lack of trust in the organisation as a result.
Both	Communications transmitted via WiFi infrastructure could be hacked or accessed inappropriately.	Communications could be intercepted.	Breach DPA, Principle 7 and Computer Misuse Act.	Reputational damage. Potential monetary penalty. Lack of trust in the organisation as a result.

Annex Five

Step Four: identify the privacy solutions

Risk (Community Cloud)	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation**: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Whole dataset could be hacked/accessed inappropriately. Personal data of approximately 20,000 individuals stored in the cloud. Data items detailed in Annex 3. No sensitive personal data as defined by the DPA 1998.	Solution provider Pinacl is accredited to ISO27001 information security management. Data storage provider Amazon meets industry best practice	Reduced	Security is in line with industry best practise. Risk is reduced to a minimum. http://pinaclsolutions.com/about
Concerns as to Principle 8, data storage outside of EEA Where is the data stored?	Community Cloud: Data is held on AWS S3 cloud storage, secured in accordance with Amazon's Security Best Practices. We currently utilise AWS's Dublin Region, which comprises 3 zones to ensure high availability.	Reduced	Security is in line with industry best practise. Risk is reduced to a minimum. EEA (of which Republic of Ireland is a member) countries have the same or similar standards of Data Protection Regulation as the UK.
Potentially, an individual's location over time could be tracked Location of an individual's device could be derived. This data is available historically and in real time.	Access to this real time data is limited to the minimum number of technical staff possible at solution provider. Access is controlled in line with ISO27001 standards. Newport City Council staff do not have access	Accept	A Minimum number of technical staff have access. The device is distinct from the individual.

	to this level of data.		
Excessive data retention How long is the data stored and what process is there to destroy?	Individual's data captured via the portal/access journey is stored for a period of 24 months. After 24 months (from last time logged in) the data is anonymised and all personal identifying elements are destroyed. Anonymising rather than deleting allows the continued use of the data aggregated statistics afterwards.	Reduced	Retention is balanced between usability for users and security of their data.
The perception may be that we are misusing customer data. Data may need to be shared with law enforcement agencies under strict conditions. Information recorded may be shared with law enforcement, governmental agencies and other authorities.	Exemptions under the DPA allow for this sharing to happen under strict conditions. Formal process to request access under section 29 Data Protection Act.	Accept	There are processes in place to manage the requests for information securely.
Data used by Service Provider The information gathered could be used by the service provider to communicate with the device holder.	There is an explicit 'Opt in' stage of the registration purposes, if a user doesn't 'Opt in' then their details are still captured for security/audit purposes, but their personal data will not be used by service provider, data will be anonymised for reporting purposes but flagged in	Reduced	Explicit opt in during registration process. Individuals can opt out at any stage. Grant conditions prohibit this in the first three years of contract.

	the systems to avoid any unwanted communication.		
Data released to third party The information stored could be sold on to a third party. Could be shared with other areas of the company/group of companies.	There is an explicit 'Opt in' stage of the registration purposes, if a user doesn't 'Opt in' then their details are still captured for security/audit purposes, but their personal data will not be released to a third party, data will be anonymised for reporting purposes but flagged in the systems to avoid any unwanted communication.	Reduced	Explicit opt in during registration process. Individuals can opt out at any stage. Grant conditions prohibit this in the first three years of contract.
Communications could be intercepted. Communications transmitted via WiFi infrastructure could be hacked or accessed inappropriately.	Public WiFi networks are typically open and do not have an SSID password or WPA encryption configured. While a home network will require you to 'share' the Public WIFI, this isn't feasible on a public network. Within a home network user access is controlled, within a public network it is open to all users. Authentication and logging is typically accomplished via some form of Radius – using defined credentials e.g. username/password or social media login details.	Reduced	Pinacl WiFi service supports VPN/security solutions across the network. Authentication is required prior to access. Pinacl disable device to device direct connections to provide protection against 'man in the middle' attacks. The Content Filter appliance (Fortinet) within the Newport public WIFi service improves security by blocking access to malicious and risky websites. It prevents malware downloads from malicious or hacked

	Pinacl also disable device to device direct connections whilst on the WiFi network to provide protection against man in the middle type attacks. There is also a general move towards websites using https: as standard method of connecting e.g. Google – which therefore implements encryption in the secure tunnel. Pinacl WiFi service supports VPN/security solutions across the network. The advice is therefore If you're accessing something sensitive via public Wi-Fi, try to do it on an encrypted website or access it via a VPN. The Content Filter appliance (Fortinet) within the Newport public WIFi service also improves security by blocking access to malicious and risky websites. It prevents malware downloads from malicious or hacked websites as well as providing highly granular blocking and filtering controls including the IWF list of sites.		websites as well as providing highly granular blocking and filtering controls including the IWF list of sites.